UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Michael A. PULLARA, Plaintiff, v. CENTRAL INTELLIGENCE AGENCY Defendant.	)	Civ. Act. No. H 99 0587

DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

Defendant, the United States Central Intelligence Agency (CIA or Agency), in accordance with Rule 56 of the Federal Rules of Civil Procedure and the Local Rules of the United States District Court for the Southern District of Texas, files its Motion for Summary Judgment in this action under the Freedom of Information Act, 5 U.S.C. § 552 (1994 & Supp. II 1996). As shown in the accompanying Memorandum of Law, there are no genuine issues of material fact and the Defendant is entitled to judgment as a matter of law.

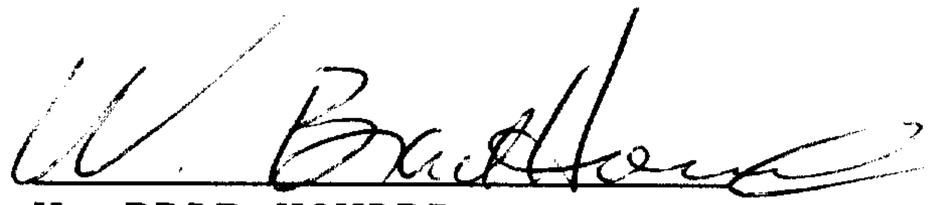
In support of this motion, Defendant relies upon the pleadings, its Memorandum of Law and the Declaration of William H. McNair, Information Review Officer (IRO) for the Directorate of Operations (DO) of the CIA ("McNair Decl."), which sets forth the administrative background regarding Plaintiff's FOIA requests, and explains why CIA can neither confirm nor deny the existence or nonexistence of records responsive to Plaintiff's requests.

#3

Based on the entire record herein and for the reasons stated in the Memorandum of Law in Support of Defendant's Motion for Summary Judgment, Defendant respectfully requests that this Motion for Summary Judgment be granted, and that judgment be entered against the Plaintiff.

Respectfully submitted,

JAMES H. DeATLEY
UNITED STATES ATTORNEY



W. BRAD HOWARD
ASSISTANT UNITED STATES ATTORNEY
State Bar No. 10082300
P.O. Box 61129
Houston, Texas 77208
Tel: (713) 567-9508
Fax: (713) 718-3303

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Michael A. PULLARA, Plaintiff, v. CENTRAL INTELLIGENCE AGENCY Defendant.	)	Civ. Act. No. H 99 0587

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

I. SUMMARY OF FACTS

1. This is an action under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (1994 & Supp. II 1996). Plaintiff submitted a FOIA request by letter dated November 4, 1997 seeking "information regarding the death of CIA Officer Fred Woodruff," an American citizen killed in Tbilisi, Georgia in 1993. By letter dated November 14, 1997, the Central Intelligence Agency ("CIA" or "Agency") acknowledged receipt of Plaintiff's FOIA request and assigned it a reference number. By letter dated July 31, 1998, CIA denied Plaintiff's FOIA request in full, pursuant to exemptions (b)(1) and (b)(3) of the FOIA.

2. CIA's July 31, 1998 letter neither confirmed nor denied the existence of records responsive to Plaintiff's FOIA request. In fact, CIA advised the Plaintiff that the fact of the existence or nonexistence of records responsive to

Plaintiff's request was itself classified pursuant to the provisions of Executive Order 12958.

3. Plaintiff appealed CIA's denial of his FOIA request by letter dated August 11, 1998. CIA denied Plaintiff's appeal by letter dated December 22, 1998. Plaintiff's lawsuit followed. The administrative treatment of Plaintiff's FOIA request is more fully described in the attached Declaration of William H. McNair ("McNair Decl.").

II. SUMMARY OF LEGAL ARGUMENT

4. This is a suit for access to records under the FOIA. Plaintiff alleges that CIA has improperly withheld records responsive to his FOIA request.

5. CIA has not improperly withheld Agency records from the Plaintiff. Whether or not records exist which are responsive to Plaintiff's FOIA request is a fact which is itself properly classified. See McNair Decl. at ¶ 16.

6. Executive Order 12958 (the "Order") governs proper classification of information and the treatment of properly classified information. Section 3.7(a) of the Order provides that any agency may refuse to confirm or deny the existence of records when that fact is, itself, classified. Information which is properly classified—such as the fact of the existence or non-existence of certain records under section 3.7(a) of the Order—is exempt from disclosure under FOIA exemption

(b)(1). Accordingly, CIA properly denied Plaintiff's FOIA request pursuant to exemption (b)(1).

7. Furthermore, Plaintiff's FOIA request seeks information on intelligence sources and methods. Under the terms of the National Security Act, 50 U.S.C. § 403-3(c)(6), the Director of Central Intelligence ("DCI") is obligated to protect intelligence sources and methods from unauthorized disclosure. Section 403g of the Central Intelligence Agency Act protects from unauthorized disclosure the identities of CIA employees. These two Acts are "withholding statutes" for purposes of FOIA exemption (b)(3), which exempts from disclosure under FOIA information "specifically exempted from disclosure by statute." Accordingly, CIA properly denied Plaintiff's FOIA request pursuant to FOIA exemption (b)(3).

III. ARGUMENT

A. Standard of Review

8. A district court reviews an agency's determination to withhold information under the FOIA de novo. 5 U.S.C. § 552(a)(4)(B). The agency bears the burden of showing that the claimed exemptions were properly invoked. Id.

9. Affidavits are sufficient to meet the government's burden if they provide an adequate factual basis for the Court's decision. Alford v. CIA, 610 F.2d 348, 349 (5th Cir.), cert. denied 449 U.S. 854 (1980). In fact, when conducting a

de novo review in the context of a national security exemption, courts "'accord substantial weight to an agency's affidavit concerning the details of the classified status of the disputed record.'" Military Audit Project v. Casey, 656 F.2d 724, 738 (D.C. Cir. 1981) (quoting Senate reports regarding FOIA provision).

10. As the Fifth Circuit Court of Appeals has held, a court should be unwilling to "second guess" the determinations by the DCI in this area, absent a showing of bad faith. Knight v. CIA, 872 F.2d 660, 664 (5th Cir. 1989), cert. denied, 494 U.S. 1004 (1990), citing CIA v. Sims, 471 U.S. 159, 179 (1985)("The decisions of the DCI, who must, of course, be familiar with the whole picture, as judges are not, are worthy of great deference given the magnitude of the national security interests and the potential risks at stake.").

B. CIA's Response to Neither Confirm Nor Deny the Existence of Responsive Records Is Proper

1. FOIA Exemption (b)(1)

11. FOIA exemption (b)(1) exempts from disclosure matters that are "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order." 5 U.S.C. § 552(b)(1).

12. Under sections 1.5(c) and 1.5(d) of Executive Order 12958 (copy attached), information is considered classified where it concerns, inter alia, intelligence activities, intelligence sources or intelligence methods or foreign relations or activities. According to section 1.2 of the Order, information fitting into one or more of these categories may be classified where the appropriate classification authority determines that the unauthorized disclosure, either by itself or in the context of other information, reasonably could be expected to cause damage to the national security that the declassification authority is able to identify and describe. In this case, the appropriate classification authority—the Agency official charged with such reviews—has determined that the very fact of the existence or nonexistence of information sought by the Plaintiff could reveal information about intelligence activities, sources and methods, including intelligence targeting, priorities and capabilities, as well as the foreign relations of the United States. Therefore, that fact is properly classified. McNair Decl. at ¶¶ 23-33.

13. As a result of this classification, the Agency's response to neither confirm nor deny the existence of responsive records is directly in accordance with section 3.7(a) of the Order, which provides that an agency may "refuse to confirm or deny the existence or nonexistence of requested

information whenever the fact of its existence or nonexistence is itself classified."

14. This standard is contained in the CIA's published regulations which advise that:

> the Agency shall decline to confirm or deny the existence or nonexistence of any responsive records whenever the fact of their existence or nonexistence is itself classified under Executive Order 12958 or revealing of intelligence sources and methods protected pursuant to section 103(c)(5)[1] of the National Security Act of 1947.

32 C.F.R. § 1900.21(c).

15. In this case, CIA properly determined that it could neither confirm nor deny the existence or non-existence of records responsive to Plaintiff's FOIA request because such a confirmation or denial would reveal classified facts, including but not limited to: (i) whether or not Woodruff was a CIA employee and (ii) whether or not Woodruff's murder, or a foreign government investigation into that murder, was of intelligence interest to the United States. Based on an admission or denial in the public record of the existence of records in this case, forces opposed to the United States or CIA would be told whether or not CIA had collected information on Woodruff's death, either as part of its own intelligence gathering mission or at the behest of other government agencies. Such information would reveal the intelligence

---

[1] Recently renumbered as section 103(c)(6).

gathering priorities of the U.S. government as well as the specific targets—or lack thereof—of U.S. intelligence missions. Such information would reveal not only the interests, but the capabilities of CIA, in support of U.S. foreign policy, to satisfy those interests.

16. Such information on foreign intelligence activities —or, again, the lack thereof— would, in turn, directly implicate information on intelligence sources and methods, as more fully described in the McNair Declaration. McNair Decl. at ¶¶ 25-28. For example, were the CIA to confirm the existence of documents indicating that it had gathered information on Woodruff's death, a hostile intelligence service would learn U.S. intelligence priorities as well as that it was the target of intelligence gathering. Indeed, the suppositions that appear to have led to Woodruff's killing (according to information supplied by the requester) would either be confirmed or disproved by an answer which admitted or denied the existence of responsive records and, thus, would directly inform foreign forces opposed to the U.S. whether their own intelligence gathering operations are successful.[2]

---

[2] According to Pullara, contemporaneous news accounts suggested that Woodruff had been assassinated by a foreign intelligence or military service because of Woodruff's alleged assistance to the Georgian intelligence or military. If this hypothesis were accurate, then for the CIA to admit or deny either that (a) Woodruff was affiliated with CIA or (b) CIA engaged in intelligence gathering to investigate Woodruff's death, would tell Woodruff's killers whether they had selected the proper target, in turn informing them of the efficacy of their own intelligence gathering sources and methods. Such information would directly impair U.S. national security, in particular, because any

In light of the foregoing, CIA accurately determined that the existence or nonexistence of records responsive to Plaintiff's FOIA request is a classified fact under the Order and is therefore exempt from disclosure pursuant to exemption (b)(1).

17. As detailed in the McNair Declaration, although the response to neither confirm nor deny the existence of records may be frustrating to a FOIA requester, it is vitally necessary to ensure that CIA does not reveal classified information simply through a pattern of responses to FOIA requests. McNair Decl. at ¶ 34. Even if CIA has no documents responsive to FOIA requests that seek classified information—such as the existence of specific intelligence targeting—the CIA cannot provide requesters with a "no records" response. Were CIA to provide a "neither confirm nor deny" response only where it had records and to provide a "no records" response where it did not have records, then a review of CIA's FOIA responses would, itself, reveal CIA intelligence priorities and missions. Because CIA will not provide a "no records" response untruthfully, i.e., where it actually has records, CIA's only protection in such circumstances is to provide the same response to all such FOIA requests, regardless of whether or not it actually possesses responsive records.

---

aid given to hostile intelligence services increases the risks of U.S. intelligence missions abroad and thus reduces their chances of success.

18. Courts have upheld CIA's position in similar circumstances. In Miller v. Casey, 730 F.2d 773 (D.C. Cir. 1984), the United States Court of Appeals for the District of Columbia Circuit upheld CIA's refusal, in response to a FOIA request, to confirm or deny the existence of records regarding alleged covert operations in Albania following World War II. The court held that "CIA's central premise—that an answer to whether the files existed would be tantamount to declaring whether the mission occurred—is . . . sound." 730 F.2d at 776. Although the events in Albania were alleged to have occurred decades prior to the FOIA request—in contrast to the present case—the court found that "CIA's claim of foreseeable harm to the national security is all but indisputable." Id. at 777. These same considerations are at play in the current litigation and support summary judgment for the Agency.

2. FOIA Exemption (b)(3)

19. Under FOIA exemption (b)(3), information that is "specifically exempted from disclosure by statute" is, under certain conditions, exempt from disclosure under the FOIA. 5 U.S.C. § 552(b)(3). In order for it to be a "withholding statute" for purposes of FOIA exemption (b)(3), a statute must "(A) require[] that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establish[] particular criteria for withholding or refer[] to particular types of matters to be withheld." Id.

20. CIA relies for its withholding in this case on section 403-3(c)(6) of the National Security Act of 1947 and section 403g of the Central Intelligence Agency Act of 1949. McNair Decl. at ¶¶ 21-22. The Supreme Court has held that both of these are "withholding statutes" for purposes of FOIA exemption (b)(3). CIA v. Sims, supra. The Supreme Court in Sims, noting the "wide-ranging authority" given to the DCI to protect intelligence sources and methods, held that it was "the responsibility of the DCI, not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk. . . ." Id. at 180. The United States Court of Appeals for the Fifth Circuit has stated unequivocally that "the FOIA simply does not apply to material the DCI specifically has exempted on the ground that it pertains to or could give rise to inferences about intelligence sources and methods." Knight, 872 F.2d at 664.

21. In this case, the CIA has determined that confirming or denying the existence of responsive records would divulge intelligence targeting, priorities and capabilities in a specific region of the world, as well as, depending on whether CIA confirmed or denied the existence of records, intelligence sources and methods. McNair Decl. at ¶¶ 29-33.

22. The information sought by Plaintiff—information that would confirm or deny the existence of an intelligence mission

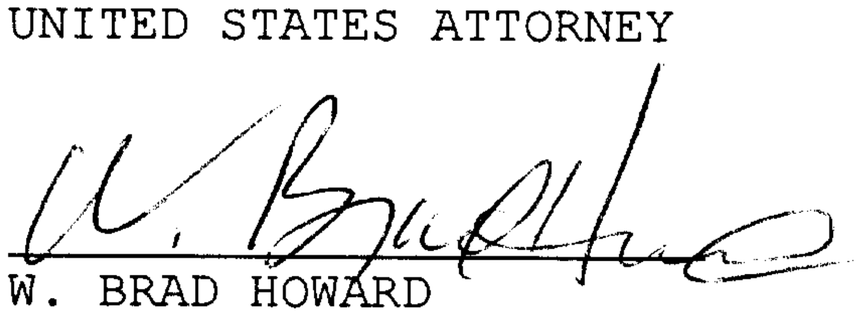
and CIA's ability to carry it out—falls squarely within the scope of the DCI's protective mandate under the National Security Act of 1947. In addition, information sought by Plaintiff would confirm or deny whether particular individuals were CIA employees, and thus falls squarely within section 6 of the Central Intelligence Agency Act of 1949. The fact of the existence or nonexistence of such information is, therefore, properly exempt from disclosure pursuant to FOIA exemption (b)(3).

IV. CONCLUSION

23. Supported by the foregoing, and the analysis set forth in the McNair Declaration, Defendant United States Central Intelligence Agency respectfully requests this Court to grant summary judgment in its favor, and dismiss Plaintiff's case with prejudice.

Respectfully submitted,

JAMES H. DeATLEY
UNITED STATES ATTORNEY



W. BRAD HOWARD
ASSISTANT UNITED STATES ATTORNEY
State Bar No. 10082300
P.O. Box 61129
Houston, Texas 77208
Tel: (713) 567-9508
Fax: (713) 718-3303

CERTIFICATE OF SERVICE

I, Brad Howard, Assistant U.S. Attorney, hereby declare that on the 31st day of March, 1999, a true and correct copy of the foregoing pleadings and proposed order was mailed to counsel of record herein via certified mail, return receipt requested, to wit:

Michael A. Pullara
1111 Hermann Drive, Suite 21A
Houston, Texas 77004

W. BRAD HOWARD
ASSISTANT U.S. ATTORNEY

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Michael A. PULLARA,	)	
	)	
Plaintiff	)	
	)	Civ. Act. No. H 99 0587
v.	)	
	)	
CENTRAL INTELLIGENCE AGENCY,	)	
	)	
Defendant.	)	
	)	
	)	

Declaration of William H. McNair

I, WILLIAM H. McNAIR, do hereby declare and say:

1. I am the Information Review Officer ("IRO") for the Directorate of Operations ("DO") of the United States Central Intelligence Agency ("CIA" or "Agency"). I have held operational and executive positions in the intelligence agencies of the United States Government since 1962, and with CIA since 1982. I served as Associate IRO from July 1993, until I was appointed to my present position in February 1994.

2. The DO is the organization within CIA responsible for the clandestine collection of foreign intelligence from human sources. As DO/IRO, I am responsible for the review of records maintained by offices in the DO that may be responsive to Freedom of Information Act ("FOIA") or Privacy Act requests, as well as to requests from the Department of

Justice in criminal and civil litigation. As part of my review of DO information, I am responsible for ensuring that any determinations as to the release or withholding of such information are proper and do not jeopardize DO interests or endanger DO personnel or facilities.

3. The authority of a CIA official to classify documents is derived from Executive Order 12958 (sometimes, hereafter, "the Order"), and predecessor orders. As a senior CIA official and pursuant to a written delegation of authority in accordance with Executive Order 12958, I hold original classification authority at the TOP SECRET level. Therefore, I am authorized to review DO information and make original classification decisions whether and to what degree that information meets the standards of the Order to be classified in the interests of national security.

4. Through the exercise of my official duties, I have become familiar with the Plaintiff's FOIA request that is the subject of this litigation. The purpose of this declaration is to explain CIA's processing of Plaintiff's FOIA request (Section I), and to detail and explain the factual basis for CIA's refusal to confirm or deny the existence or nonexistence of records responsive to that request (Sections II & III).

5. The statements made herein are based upon my personal knowledge, information made available to me in my

official capacity, the advice and counsel of the CIA Office of General Counsel, and my conclusions and determinations in accordance therewith.

I. PROCESSING OF PLAINTIFF'S FOIA REQUEST

6. By a letter dated November 4, 1997, Plaintiff Michael Pullara submitted a FOIA request seeking "information regarding the death of CIA Officer Fred Woodruff." Plaintiff indicated that his request included, but was not limited to, documents relating or referring to "(i) any investigation(s) of Woodruff's death; (ii) any evidence adduced in such investigation(s); and (iii) any reports generated and conclusions reached in connection with such investigation(s)."

7. By letter dated November 14, 1997, CIA acknowledged receipt of Plaintiff's FOIA request and assigned it reference number F-1997-02637.

8. By letter dated July 31, 1998, CIA denied Plaintiff's FOIA request, pursuant to FOIA exemptions (b)(1) and (b)(3), to the extent that the request might concern records either (a) containing information that would divulge the identity of an unacknowledged employee or (b) divulge a covert Agency affiliation.

9. CIA's July 31 letter clearly stated that by denying Plaintiff's FOIA request, CIA was neither confirming nor denying that any such information existed.

10. By letter dated August 11, 1998, Plaintiff appealed CIA's denial of his FOIA request. In this letter, Plaintiff stated he believed "there has been official acknowledgment of (i) Woodruff's affiliation with the Agency; and (ii) the fact that he was acting in an official capacity at the time of his death." Plaintiff, however, continued his appeal letter by stating his belief that "the Agency can fully respond to my request without confirming or denying Woodruff's affiliation or mission status." He offered that "[t]o the extent that [Woodruff's] affiliation or status may be disclosed in an Agency document, these references can be expurgated."

11. By letter dated September 18, 1998, CIA accepted Plaintiff's appeal.

12. By letter dated December 22, 1998, CIA denied Plaintiff's appeal. This letter advised Plaintiff that the Information Review Officer had determined that "the fact of the existence or nonexistence of any documents which would be responsive to [Plaintiff's] request is classified pursuant to Executive Order 12958."

13. On February 25, 1999, Plaintiff filed the present law suit.

II. APPLICABLE FOIA EXEMPTIONS

14. CIA's determination to neither confirm nor deny the existence of records responsive to Plaintiff's FOIA request is based on exemptions (b)(1) and (b)(3) of the FOIA. These provisions are summarized in this Section and then applied to Plaintiff's request in Section III.

A. FOIA Exemption (b)(1)

15. FOIA exemption (b)(1), 5 U.S.C. § 552(b)(1), provides that the disclosure provisions of the FOIA do not apply to matters that are:

> (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order.

16. Executive Order 12958 at § 1.5 specifies categories of information that are eligible for classification. One such category of information is that which concerns intelligence activities or intelligence sources or methods. Id. at § 1.5(c). Moreover, § 1.2 of the Order provides that information falling within one of those categories may be classified when, inter alia, an "original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify

and describe the damage." I have determined, and consistently maintained, that disclosure of the mere fact of whether or not CIA possesses records pertaining to the death of Mr. Woodruff and any investigation into that death would tend to reveal intelligence activities, sources and methods and cause damage to the national security. I am able to identify and describe that damage and will do so in this Declaration. The Agency's possession or not of records responsive to Plaintiff's FOIA request is, therefore, properly classified.

17. Generally, the CIA responds to a FOIA request for information on a particular subject by either providing or not providing the requested records. In this typical situation, the CIA's answer, either to provide or not provide the records sought, actually confirms to the requester (and the world, for that matter) the existence or non-existence of such CIA records. However, where appropriate, as is the case here, pursuant to section 3.7(a) of the Order, the Agency "may refuse to confirm or deny the existence or non-existence of requested information whenever the fact of its existence or non-existence is itself classified under this order." Such a classified fact, therefore, is also subject to FOIA exemption (b)(1).

18. In addition to intelligence activities and intelligence sources and methods, the foreign relations or

foreign activities of the United States comprise another category of information eligible for classification as provided at § 1.5(d) of Executive Order 12958.

19. Though it is known that the CIA collects intelligence on foreign countries, identifying an intelligence interest in a particular activity in a particular country cannot even be implied. An official acknowledgment that the CIA maintains information on a particular activity, individual or entity, can be tantamount to a CIA admission that it has collected or is attempting to collect information on that activity, individual, or entity. This reveals that CIA is targeting intelligence sources and methods, or attempting to develop or recruit intelligence sources, at people and entities with access to that specific information during specific time periods. As described above, such an admission by this Agency invariably would affect the United States' foreign relations and foreign activities by triggering a negative diplomatic or economic response by one or more countries or even retaliation against American interests in a given region.

B. FOIA Exemption (b)(3) Statutory Protection of Information (National Security Act of 1947 and Central Intelligence Agency Act of 1949)

20. The existence or nonexistence of records responsive to Plaintiff's FOIA request is also properly exempt from disclosure pursuant to FOIA exemption (b)(3).

21. Exemption (b)(3) of the FOIA provides that the disclosure provisions of the FOIA do not apply to matters that are:

> specifically exempted from disclosure by statute ... provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

Section 103(c)(6) of the National Security Act of 1947, as amended,[1] requires the Director of Central Intelligence to protect intelligence sources and methods from unauthorized disclosure. As described above, the CIA can neither confirm nor deny that it maintains records concerning a covert or clandestine interest in an individual or subject matter because to do so could divulge intelligence sources and methods. This is the only way that the CIA can continue to fulfill its intelligence responsibilities against groups who seek to learn about the CIA's intelligence sources and methods and their application.

---

[1] Codified at 50 U.S.C. § 403-3(c)(6).

22. In addition, the names and official titles of CIA employees are exempted from disclosure by section 6 of the Central Intelligence Agency Act of 1949, as amended, 50 U.S.C. 403g.

III. CIA's DETERMINATION THAT THE EXISTENCE OR NONEXISTENCE OF RESPONSIVE RECORDS IS, ITSELF, CLASSIFIED

23. Plaintiff seeks information that would disclose (a) the existence or non-existence of a CIA relationship with a named U.S. citizen; and (b) the existence or non-existence of a CIA intelligence collection target—any investigation into the killing of that U.S. citizen abroad.

24. The fact of the existence or nonexistence of records containing such information, irrespective of the content of such supposed records, is so intricately intertwined with intelligence activities, intelligence sources and methods and foreign relations of the United States that this fact itself is classified pursuant to § 1.5(c) (intelligence activities, sources and methods) and § 1.5(d) (foreign relations) of Executive Order 12958, and, with respect to Woodruff, by the Director of Central Intelligence's legal obligation pursuant to § 103(c)(6) of the National Security Act of 1947 to protect intelligence sources and methods from unauthorized disclosure.

A. Intelligence Sources and Methods Classified Relationships

25. CIA is charged with protecting the sources and methods used to carry out its foreign intelligence and counterintelligence collection and analysis responsibilities. The CIA utilizes both United States citizens and foreign nationals to collect intelligence directly, to spot or provide access to others who may have intelligence information, or to support our intelligence collection activities. If the CIA were to provide a response to Plaintiff that either confirms or denies that it possesses records responsive to its requests, this would, in effect, be an official acknowledgment of whether CIA had an intelligence relationship with the subject of the requests, Fred Woodruff.

26. Disclosure of the identity of covert CIA employees reasonably could be expected to cause damage to the national security by impeding intelligence gathering activities. Many of the CIA's employees gather intelligence by working in a covert capacity in clandestine locations overseas. In order for CIA officers to effectively collect intelligence around the world, they cannot acknowledge publicly that they work for CIA and, conversely, CIA cannot acknowledge a particular individual's affiliation with it. Consequently, in carrying out its statutory mission of gathering intelligence for dissemination to government policy makers,

the CIA employs a variety of cover mechanisms in order to effectively collect intelligence. These cover mechanisms are necessary to the security of past, present and future operations in which these, or other, officers participate. This is no less true when a covert employee retires, dies or leaves the Agency. His or her prior affiliation with CIA is normally still classified in order to protect that officer's former contacts, the CIA facilities at which he or she was stationed, the cover mechanisms employed to protect his or her affiliations with CIA, and the operations which he or she conducted.

27. Additionally, the public disclosure of an individual's affiliation with CIA could and, in fact, has threatened the safety and lives of not only the officer, but also their families, colleagues, officials of foreign governments, and other foreign nationals with whom they had, either wittingly or unwittingly, contact. Individuals associated with CIA have been and will continue to be subjected to threats, reprisals and physical injuries from foreign intelligence services, terrorist groups, and other persons or organizations hostile to CIA or the United States government. Should CIA covert employees believe that the Agency was incapable of protecting their identity, they would likely be unwilling to undertake the personal risks which are associated with their employment with CIA. It is

for these reasons that the names of specific CIA employees who work or have worked under cover are properly classified pursuant to E.O. 12958 and specifically protected from public disclosure by 50 U.S.C. §403g and, thus, are exempt from FOIA disclosure.

28. Conversely, CIA cannot acknowledge when a particular individual does not work for the CIA as this reasonably could be expected to cause damage to the national security. Hostile intelligence services seek to identify those Americans working in a particular location who are, in fact, covert CIA employees. The hostile service can focus its resources on surveilling those individuals and watching with whom they meet, and monitoring their activities. In this way, a hostile service can identify, assess, and/or take countermeasures against CIA intelligence gathering activities. Should the CIA publicly acknowledge which particular individuals are not employed with the Agency, then this would allow hostile services to redirect their resources on other individuals who may, in fact, really be working for the CIA. In addition, a refusal to confirm or deny whether or not someone had a classified relationship with CIA is effective only when done both when there is and when there is not such a relationship.

B. Intelligence Activities Existence or Non-existence of CIA Intelligence Collection Targets

29. The CIA is charged with both foreign intelligence and counterintelligence collection and analysis responsibilities. While it is obviously widely acknowledged that CIA is responsible for performing activities in support of this mission for the United States, CIA cannot confirm or deny the existence of any specific intelligence operation or disclose the target or targets of such intelligence gathering activities.

30. To disclose the existence or non-existence of a particular intelligence mission would reveal U.S. intelligence needs, priorities and capabilities. If, for example, CIA were to admit that it did have records responsive to Plaintiff's FOIA request, it would be an admission that Woodruff's death was a topic of foreign intelligence interest.[2] If so, CIA would have pursued collecting information through the application of classified intelligence sources and methods. Therefore, were CIA to admit the existence of records, it would be admitting that it had applied intelligence sources and methods in a

---

[2] The fact that Woodruff was an American citizen who was the victim of a crime abroad would not alone be sufficient to generate CIA reporting or a CIA investigation. By statute, CIA has no law enforcement investigation authority. 50 U.S.C. § 403-3(d)(1). Therefore, CIA would have collected information on Woodruff's death only to the extent that his murder was of foreign intelligence interest.

particular region against particular targets in furtherance of an admitted intelligence mission.

31. The damage that would be caused by such an admission is clear. Not only would foreign government services be advised that their activities and information had been targeted by the CIA, they would learn from the amount of responsive records CIA's collection abilities and priorities. Future intelligence collection operations would be made more difficult by such a revelation and, as a result, the conduct of such operations would become even more dangerous. In this case, the degree of damage would be magnified because the topic of interest is so narrow that only select persons and foreign government entities would have access to information.

32. If, on the other hand, CIA denied the existence of responsive records, this would also reveal extremely sensitive information to hostile countries and intelligence services. If CIA were to admit that it had no records regarding Woodruff's death, i.e., that his killing was not of foreign intelligence interest, it would provide information on U.S. intelligence priorities and interests, as well as CIA resources or capabilities to conduct an intelligence collection activity in a particular region on a particular topic. Finally, of course, CIA's refusal to confirm or deny must be consistently used to remain viable.

33. Furthermore, I have determined that official acknowledgment of whether or not CIA has information on any investigation into the death of Mr. Woodruff could reasonably be expected to harm the foreign relations of the United States. Should CIA have information on an investigation conducted by a foreign government entity, that revelation would tend to reveal to the foreign government that CIA had conducted clandestine intelligence collection activities targeted at officials of that foreign government, possibly by recruiting one of that government's own officials to be an intelligence source for CIA. If that foreign government had willingly shared information about its investigation with CIA, that sharing would have occurred in the context of an intelligence liaison relationship. Therefore, CIA's revelation that it possessed records would be perceived as a breach of the Agency's commitment to keep secret any information shared with it by a liaison service. Such perceptions could be expected to harm the foreign relations and foreign activities of the United States.

IV. CONCLUSION

34. CIA must respond in a consistent manner to all FOIA requests that on their face seek information the existence or nonexistence of which is classified. To neither confirm nor deny the existence of records responsive

to such FOIA requests is the best protection to the security of the CIA's operations and preserves the confidential nature of intelligence sources and methods. Were the CIA to deny that it maintains responsive information in cases where the CIA did not possess such information, then the CIA response that refuses to confirm or deny whether the CIA has information would be tantamount to admitting that the CIA, in fact, possesses such information. Such a policy in responding to such FOIA requests obviously would reveal the very information that the CIA is attempting to protect (i.e., the existence of a specific intelligence gathering effort), would provide a valuable advantage to foreign intelligence services, and would unduly jeopardize the CIA's intelligence activities worldwide. Were the CIA simply to admit that it maintains records but refuse to produce them, this would also disclose the very fact that CIA must protect. Therefore, when CIA receives such a FOIA request, CIA will neither confirm nor deny the existence of responsive records, whether or not the Agency actually possesses responsive records.

35. The circumstances described in Plaintiff's FOIA request are themselves an example of precisely the severe harms that CIA's position seeks to avoid. As described in Plaintiff's FOIA request and the contemporaneous news accounts he enclosed, when a foreign country's intelligence

service believes that CIA is providing aid to another country's intelligence service, personnel alleged to be associated with CIA are placed in jeopardy of their lives. It is for precisely this reason that CIA cannot disclose the existence or nonexistence of particular intelligence operations or the affiliation or nonaffiliation with CIA of any specific person. Plaintiff's FOIA request requires this result.

36. In sum, I have determined that the very fact of whether CIA records exist which would be responsive to Plaintiff's requests is currently and properly classified pursuant to Executive Order 12958 and would reveal information about CIA intelligence sources and methods which the Director of Central Intelligence is obligated to protect from disclosure pursuant to the National Security Act of 1947 and the Central Intelligence Agency Act of 1949. As such, the only appropriate response to this request is for CIA to neither confirm nor deny the existence or nonexistence of such records pursuant to FOIA exemptions (b)(1) and (b)(3).

I DECLARE UNDER PENALTY OF PERJURY THAT THE FOREGOING IS TRUE AND CORRECT.

Executed on this 30 day of March 1999.

William H. McNair

ull-time staff and consultants as authorized by the

esident reports of intelligence activities that the IOB or contrary to Executive order or Presidential direc-

orney General reports received concerning intelligence ieves may be unlawful or contrary to Executive order

l guidelines of each agency within the Intelligence ne lawfulness of intelligence activities;
s and procedures of the Inspectors General and Gen- gence Community for discovering and reporting intel- be unlawful or contrary to Executive order or Presi-

igations as the IOB deems necessary to carry out its

hen required by this order, report to the President FIAB. The IOB shall consider and take appropriate dentified by the Director of Central Intelligence, the other agencies of the Intelligence Community. With opriate by the President, the IOB shall advise and tions to the Director of Central Intelligence, the other agencies of the Intelligence Community.

tments and agencies of the Intelligence Community, shall provide the IOB with all information that the ut its responsibilities. Inspectors General and Gen- Community, to the extent permitted by law, shall quarterly basis and from time to time as necessary ligence activities that they have reason to believe xecutive order or Presidential directive.

III. General Provisions

available to the PFIAB, or members of the PFIAB ll be given all necessary security protection in ac- nd regulations. Each member of the PFIAB, each l each of the PFIAB's consultants shall execute an ssified information obtained by virtue of his or her the President or to such persons as the President

AB shall serve without compensation but may re- l per diem allowance as authorized by law. Staff ll receive pay and allowances as authorized by the

12334 of December 4, 1981, as amended, and Ex- r 28, 1985, as amended, are revoked.

WILLIAM J. CLINTON

EXECUTIVE ORDER NO. 12958 CLASSIFIED NATIONAL SECURITY INFORMATION

(April 17, 1995, 76 F.R. 19825)

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—ORIGINAL CLASSIFICATION

Section 1.1. *Definitions.* For purposes of this order:

(a) "National security" means the national defense or foreign relations of the United States.

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(d) "Foreign Government Information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, and any other entity within the executive branch that comes into the possession of classified information.

(j) "Senior agency official" means the official designated by the agency head under section 5.6(c) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Sec. 1.2. *Classification Standards.* (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;

(2) the information is owned by, produced by or for, or is under the control of the United States Government;

(3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and

(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Sec. 1.3. *Classification Levels.* (a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.4. *Classification Authority.* (a) The authority to classify information originally may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the Federal Register; or

(3) United States Government officials delegated this authority pursuat to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Ori
tion as prov
(e) Exc
or grantee
nates inforr
shall be pro
rectives. Th
order or its
ter interest
cy shall deci
which agenc
to the Direct
termine the
mation, with
mination.

Sec. 1.5.
Informat
(a) milita
(b) foreig
(c) intelli
methods, or c
(d) foreig
fidential sourc
(e) scienti
rity;
(f) United
facilities; or
(g) vulner
lating to the n

Sec. 1.6. *L*
original classif
for declassifica
the informatio
(b), below.
(b) If the
date or event
10 years from t
below.
(c) An origi
or reclassify spe
time if such ac
under this orde
that are more th
torical value unc
(d) At the ti
exempt from dec
disclosure of wh
security for a pe
release of which
(1) revea
or activity;
(2) revea
ons of mass c
(3) revea
nology within
(4) revea
paredness pla
(5) reveal
(6) damag
reveal a confi
are reasonabl
in paragraph
(7) impair
protect the Pr
tection service
(8) violate a st

ny individual or organization that has pro-
ected to provide, information to the United
tional security with the expectation that the
e to be held in confidence.
y" means harm to the national defense or for-
n the unauthorized disclosure of information,
ility of that information.

. (a) Information may be originally classified
l of the following conditions are met:
uthority is classifying the information;
by, produced by or for, or is under the control

n one or more of the categories of information
and
authority determines that the unauthorized
onably could be expected to result in damage
riginal classification authority is able to iden-

bout the need to classify information, it shall
ot:
bstantive criteria or procedures for classifica-

procedural rights subject to judicial review.
ot be declassified automatically as a result of
al or similar information.

a) Information may be classified at one of the

lied to information, the unauthorized disclosure
pected to cause exceptionally grave damage to
ginal classification authority is able to identify

to information, the unauthorized disclosure of
ted to cause serious damage to the national se-
ation authority is able to identify or describe.
pplied to information, the unauthorized disclo-
e expected to cause damage to the national se-
ation authority is able to identify or describe.
d by statute, no other terms shall be used to
rmation.
about the appropriate level of classification, it

y. (a) The authority to classify information origi-

als designated by the President in the Federal

ent officials delegated this authority pursuat to

ify information at a specified level are also au-
lower level.
ication authority.
classification authority shall be limited to the
er this order. Agency heads are responsible for
dinate officials have a demonstrable and continu-
ity.
lassification authority may be delegated only by
nead or official designated pursuant to paragraph

al" original classification authority may be dele-
n agency head or official designated pursuant to
senior agency official, provided that official has
iginal classification authority by the agency head.
ginal classification authority shall be in writing
e redelegated except as provided in this order.
the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

(e) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.5. *Classification Categories.*
Information may not be considered for classification unless it concerns:
(a) military plans, weapons systems, or operations;
(b) foreign government information;
(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
(d) foreign relations or foreign activities of the United States, including confidential sources;
(e) scientific, technological, or economic matters relating to the national security;
(f) United States Government programs for safeguarding nuclear materials or facilities; or
(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Sec. 1.6. *Duration of Classification.* (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

(1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair the development or use of technology within a United States weapons system;

(4) reveal United States military plans, or national security emergency preparedness plans;

(5) reveal foreign government information;

(6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;

(7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or
(8) violate a statute, treaty, or international agreement.

(e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.7. *Identification and Markings.* (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.3 of this order;

(2) the identity, by name or personal identifier and position, of the original classification authority;

(3) the agency and office of origin, if not otherwise evident;

(4) declassification instructions, which shall indicate one of the following:

(A) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or

(B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or

(C) the exemption category from declassification, as prescribed in section 1.6(d); and

(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.

(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Sec. 1.8. *Classification Prohibitions and Limitations.* (a) In no case shall information be classified in order to:

(1) conceal violations of law, inefficiency, or administrative error;

(2) prevent embarrassment to a person, organization, or agency;

(3) restrain competition; or

(4) prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

duration of classification under prede-
cy's Determination Required," or infor-
at contains no declassification instruc-
part 3 of this order.

) At the time of original classification,
ch classified document, or shall be ap-
ate manner:
vels defined in section 1.3 of this order;
l identifier and position, of the original

not otherwise evident;
ch shall indicate one of the following:
sification, as prescribed in section 1.6(a)

om the date of original classification, as

m declassification, as prescribed in sec-

on which, at a minimum, cites the appli-
1.5 of this order.
aragraph (a), above, may be excluded if
tion.
marking or other means, indicate which
classification level, which portions are ex-
6(d) of this order, and which portions are
prescribed in directives issued under this
urity Oversight Office may grant waivers
f documents or information. The Director

abuse.
ions of this order, including abbreviations
l working papers, shall conform to the
ctives issued pursuant to this order.
nall retain its original classification mark-
ation that provides a degree of protection
he entity that furnished the information.
ssification under this or predecessor orders
level of classification despite the omission
uch information is used in the derivative
ossible declassification, holders of such in-
priate classification authority for the appli-

whenever practicable, use a classified ad-
constitutes a small portion of an otherwise

and Limitations. (a) In no case shall infor-

fficiency, or administrative error;
person, organization, or agency;

of information that does not require protec-
ity.
tion not clearly related to the national secu-

sified after it has been declassified and re-
rity.
usly been disclosed to the public under prop-
sified after an agency has received a request
on Act (5 U.S.C. 552) or the Privacy Act of
review provisions of section 3.6 of this order
quirements of this order and is accomplished
the personal participation or under the di-
agency head, or the senior agency official des-
r. This provision does not apply to classified
are more than 25 years old and have been de-
value under title 44, United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and

(2) is not otherwise revealed in the individual items of information.

As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Sec. 1.9. *Classification Challenges.* (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

PART 2—DERIVATIVE CLASSIFICATION

Sec. 2.1. *Definitions.* For purposes of this order: (a) "Derivative classification" means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(c) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

Sec. 2.2. *Use of Derivative Classification.* (a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

(B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.3. *Classification Guides.* (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.

PART 3—DECLASSIFICATION AND DOWNGRADING

Sec. 3.1. DEFINITIONS. For purposes of this order: (a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(c) "Declassification authority" means:

(1) the official who authorized the original classification, if that official is still serving in the same position;

(2) the originator's current successor in function;

(3) a supervisory official of either; or

(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(h) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Sec. 3.2. *Authority for Declassification.* (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Sec. 3.3. *Transferred Information.* (a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order.Such information may be declassified or downgraded by the agency in posses-

AND DOWNGRADING

poses of this order: (a) "Declassification" means of information from classified information to un-

means the declassification of information based

cific date or event as determined by the original

ximum time frame for duration of classification

means:
ized the original classification, if that official is
on;
successor in function;
either; or
lassification authority in writing by the agency
ial.
review" means the review for declassification of
o a request for declassification that meets the re-
s order.
review" means the review for declassification of
records that have been determined by the Archi-
st") to have permanent historical value in accord-
nited States Code.
ans written instructions issued by a declassifica-
ements of information regarding a specific subject
ements that must remain classified.
etermination by a declassification authority that
arded at a specified level shall be classified and

entary material, regardless of its physical form or
n accordance with a filing system or maintained
e same function or activity.

sification. (a) Information shall be declassified as
ndards for classification under this order.
nation that continues to meet the classification re-
quires continued protection. In some exceptional
t such information may be outweighed by the pub-
information, and in these cases the information
ch questions arise, they shall be referred to the
official. That official will determine, as an exercise
nterest in disclosure outweighs the damage to na-
nably be expected from disclosure. This provision

e substantive criteria or procedures for classifica-

e or procedural rights subject to judicial review.
rmation Security Oversight Office determines that
ion of this order, the Director may require the in-
the agency that originated the classification. Any
y be appealed to the President through the Assist-
al Security Affairs. The information shall remain
ion on the appeal.
ction shall also apply to agencies that, under the
original classification authority, but had such au-

mation. (a) In the case of classified information
a transfer of functions, and not merely for storage
nall be deemed to be the originating agency for pur-

information that is not officially transferred as de-
but that originated in an agency that has ceased
no successor agency, each agency in possession of
d to be the originating agency for purposes of this
leclassified or downgraded by the agency in posses-

sion after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

Sec. 3.4. *Automatic Declassification.* (a) Subject to paragraph (b), below, within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

(1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;

(2) reveal information that would assist in the development or use of weapons of mass destruction;

(3) reveal information that would impair U.S. cryptologic systems or activities;

(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) reveal actual U.S. military war plans that remain in effect;

(6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;

(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or

(9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the file series;

(2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the information;

(2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and

(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

Sec. 3.5. *Systematic Declassification Review.* (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist of the shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives as of the effective date of this order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

ɔrmation is automatically declassified under this
gency official shall notify the Director of the In-
e, serving as Executive Secretary of the Inter-
eals Panel, of any specific information beyond
e President under paragraph (c), above, that the
omatic declassification. The notification shall in-

ɔmation;
he information is exempt from automatic declas-
ɔified for a longer period of time; and
f a confidential human source or a human intel-
ɔaragraph (b), above, a specific date or event for
ion. The Panel may direct the agency not to ex-
lassify it at an earlier date than recommended.
uch a decision to the President through the As-
tional Security Affairs. The information will re-
ɔpeal is pending.
date of this order, the agency head or senior
rector of the Information Security Oversight Of-
ɔ the requirements of this section, including the
es. Each such plan shall include the requirement
15 percent of the records affected by this section
ive date of this order, and similar commitments
ive date for automatic declassification.
ɔ automatic declassification under this section
ory and systematic declassification review provi-

determine when the United States should com-
priate officials of a foreign government or inter-
its to modify any treaty or international agree-
n of information contained in records affected by
n 25 years from the date of its creation, unless
ent pertains to information that may otherwise
nder this section.

cation Review. (a) Each agency that has origi-
this order or its predecessors shall establish and
leclassification review. This program shall apply
mpted from automatic declassification under sec-
nall prioritize the systematic review of records

e Information Security Policy Advisory Council,
is order, on specific subject areas for systematic

ɛr interest and the likelihood of declassification

conduct a systematic declassification review pro-
accessioned into the National Archives as of the
rmation transferred to the Archivist pursuant to
ɪtes Code; and (3) information for which the Na-
ɪistration serves as the custodian of the records
has gone out of existence. This program shall
- than 25 years from the date of their creation.
ɪities for the systematic review of these records
f the Information Security Policy Advisory Coun-
ɛrest and the likelihood of declassification upon
ɪiewed in accordance with the standards of this
and declassification guides provided to the Archi-
the records. The Director of the Information Se-
-e that agencies provide the Archivist with ade-
ɪuides.
ɛcted agencies, the Secretary of Defense may es-
ɪtematic review for declassification of classified
ɪirector of Central Intelligence may establish spe-
iew for declassification of classified information
ɛs (including special activities), or intelligence

Sec. 3.6. *Mandatory Declassification Review.* (a) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and

(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by:

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or

(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

Sec. 3.7. *Processing Requests and Reviews.* In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents in the process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.8. *Declassification Database.* (a) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Governmentwide database of informa-

tion that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

PART 4—SAFEGUARDING

Sec. 4.1. *Definitions.* For purposes of this order: (a) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(b) "Access" means the ability or opportunity to gain knowledge of classified information.

(c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) "Network" means a system of two or more computers that can exchange data or information.

(g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Sec. 4.2. *General Restrictions on Access.* (a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(f) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside

any otl
origina
ment fc
tion, th

Sec
distribu
tions or
tion.

(b)
curring
cooperat
distribut

Sec.
Unless ot
and Ene
each, ma
to intellig
ational, s
function
shall keep
lish them

(1
(2
format
inform
(3
(b) *Req*
(1)
ber of
mensur
tion inv
(2)
for spec
order.
(3)
lished u
tion Sec
cordance
the func
order. A
rector an
sight Off
and vuln
(4) T
access pr
this order
(5) U
National
special ac
(c) Within
principal depu
jurisdiction. Th
clearly meet th
an agency hea
lished on the ef
(d) Nothing
10 U.S.C. 119.

Sec. 4.5. *A*
(a) The requirer
mation may be g
may be waived f
(1) are e
(2) previ
pointed by th
(b) Waivers
agency official of

st shall also explore other possible uses
n process.
ith the Archivist in these efforts.
warranted by law, all declassified infor-
olished under paragraph (a), above, shall

of this order: (a) "Safeguarding" means
to protect classified information.
tunity to gain knowledge of classified in-

nation made by an authorized holder of
ecipient requires access to specific classi-
ssist in a lawful and authorized govern-

neans an assembly of computer hardware,
t, create, communicate, compute, dissemi-
rmation.
xists when information is unchanged from
or intentionally modified, altered, or de-

or more computers that can exchange data

preparation, transmission, or communica-

a program established for a specific class
eguarding and access requirements that ex-
tion at the same classification level.

ess. (a) A person may have access to classi-

eligibility for access has been made by an
signee;
proved nondisclosure agreement; and
w the information.
main under the control of the originating
agency shall not disclose information origi-
ut its authorization. An official or employee
classified information from the agency's con-

be removed from official premises without

ate classified information outside the execu-
of the information in a manner equivalent
anch.
, and regulation, an agency head or senior
procedures to ensure that automated informa-
elecommunications systems, that collect, cre-
ate, process, or store classified information

ized persons; and
information.
, and regulation, each agency head or senior
to ensure that classified information is used,
tted, and destroyed under conditions that pro-
access by unauthorized persons.
sued pursuant to this order, an agency shall
ition under standards that provide a degree of
required by the government or international
rnished the information. When adequate to
may be less restrictive than the safeguarding
nited States "Confidential" information, includ-
h a need-to-know who have not otherwise been
nation or executed an approved nondisclosure

te or directives issued pursuant to this order,
one agency may not be disseminated outside

any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

Sec. 4.3. *Distribution Controls.* (a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.4. *Special Access Programs.* (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or

(3) the program is required by statute.

(b) *Requirements and Limitations.*

(1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.6(c) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

(c) Within 180 days after the effective date of this order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this order. Each existing special access program that an agency head or principal deputy validates shall be treated as if it were established on the effective date of this order.

(d) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.5. *Access by Historical Researchers and Former Presidential Appointees.* (a) The requirement in section 4.2(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects; or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

PART 5—IMPLEMENTATION AND REVIEW

Sec. 5.1. *Definitions.* For purposes of this order: (a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(b) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(c) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a "violation," as defined above.

Sec. 5.2. *Program Direction.* (a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

(1) classification and marking principles;

(2) agency security education and training programs;

(3) agency self-inspection programs; and

(4) classification and declassification guides.

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information.

Sec. 5.3. *Information Security Oversight Office.* (a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director ofthe Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;

ıccess is consistent with the interest of na-

rotect classified information from unauthor-
ensures that the information is safeguarded
ler; and
former Presidential appointees to items that
gned, or received while serving as a Presi-

REVIEW

of this order: (a) "Self-inspection" means the
vidual agency activities and the agency as a
ıtion of the program established under this

ent action that could reasonably be expected
of classified information;
gligent action to classify or continue the clas-
to the requirements of this order or its imple-

egligent action to create or continue a special
juirements of this order.
ıg, willful, or negligent action contrary to the
lementing directives that does not comprise a

The Director of the Office of Management and
stant to the President for National Security Af-
ty Policy Board, shall issue such directives as
er. These directives shall be binding upon the
rector of the Office of Management and Budget

g principles;
ı and training programs;
ɔgrams; and
ification guides.
Management and Budget shall delegate the im-
ıons of this program to the Director of the Infor-

stablished by a Presidential Decision Directive,
e President through the Assistant to the Presi-
vith respect to the issuance of a Presidential di-
ıformation. The Presidential directive shall per-
ibution, transmittal, and destruction of and ac-

Oversight Office. (a) There is established within
get an Information Security Oversight Office. The
ent and Budget shall appoint the Director of the
ice, subject to the approval of the President.
Director of the Office of Management and Budget
sistant to the President for National Security Af-
ɔn Security Oversight Office shall:
he implementation of this order;
to ensure compliance with this order and its im-

ency implementing regulations and agency guides
review prior to their issuance by the agency;
conduct on-site reviews of each agency's program
and to require of each agency those reports, infor-
n that may be necessary to fulfill its responsibil-
specific categories of classified information would
security risk, the affected agency head or the sen-
ıit a written justification recommending the denial
e Office of Management and Budget within 60 days
cess shall be denied pending a prompt decision by
Management and Budget, who shall consult on this
ɔ the President for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Director of the Office of Management and Budget;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.4. *Interagency Security Classification Appeals Panel.* (a) Establishment and Administration.

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) *Functions.* The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.4 of this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order.

(c) *Rules and Procedures.* The Panel shall issue bylaws, which shall be published in the Federal Register no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which:

(1) the appellant has exhausted his or her administrative remedies within the responsible agency;

(2) there is no current action pending on the issue within the federal courts; and

(3) the information has not been the subject of review by the federal courts or the Panel within the past 2 years.

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs.The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

Sec. 5.5. *Information Security Policy Advisory Council.* (a) Establishment. There is established an Information Security Policy Advisory Council ("Council"). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from among persons who have demonstrated in-

terest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council Chair from among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C.App. 2.

(b) *Functions*. The Council shall:

(1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policiesestablished under this order or its implementing directives, including recommended changes to those policies;

(2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) *Meetings*. The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

(d) *Administration*.

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) To the extent permitted by law and subject to the availability of funds, the Information Security Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the Congress, shall be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

Sec. 5.6. *General Responsibilities*. Heads of agencies that originate or handle classified information shall: (a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order; (b) commit necessary resources to the effective implementation of the program established under this order; and (c) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programsauthorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access toclassified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information; (8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the

d to the subject matter of this order and are
al Government. The President shall appoint
nbers. The Council shall comply with the Fed-
ded, 5 U.S.C.App. 2.

Assistant to the President for National Secu-
fice of Management and Budget, or such other
ems appropriate, on policiesestablished under
lirectives, including recommended changes to

to agency heads for specific subject areas for
; and
is policy issues in dispute.
neet at least twice each calendar year, and as
President for National Security Affairs or the
and Budget.

ıay be compensated at a rate of pay not to ex-
annual rate of basic pay in effect for grade GS-
er section 5376 of title 5, United States Code,
member is engaged in the actual performance

ıomes or regular place of business in the actual
ıe Council, members may be allowed travel ex-
ieu of subsistence, as authorized by law for per-
ıe Government service (5 U.S.C. 5703(b)).
l by law and subject to the availability of funds,
ight Office shall provide the Council with admin-
iff, and other support services necessary for the

ther Executive order, the functions of the Presi-
ry Committee Act, as amended, that are applica-
of reporting to the Congress, shall be performed
tion Security Oversight Office in accordance with
established by the General Services Administra-

ities. Heads of agencies that originate or handle
monstrate personal commitment and commit sen-
implementation of the program established under
resources to the effective implementation of the
rder; and (c) designate a senior agency official to
ı, whose responsibilities shall include:
's program established under this order, provided,
ıate a separate official to oversee special access
iis order. This official shall provide a full account-
cess programs at least annually;
ıenting regulations, which shall be published in the
ıt that they affect members of the public;
ntaining security education and training programs;
ıntaining an ongoing self-inspection program, which
view and assessment of the agency's classified prod-

res to prevent unnecessary access to classified infor-
s that: (i) require that a need for access toclassified
efore initiating administrative clearance procedures;
nber of persons granted access to classified informa-
ıum consistent with operational and security require-

contingency plans for the safeguarding of classified
- hostile or potentially hostile areas;
erformance contract or other system used to rate ci-
l performance includes the management of classified
lement or item to be evaluated in the rating of: (i)
ıorities; (ii) security managers or security specialists;
ıel whose duties significantly involve the creation or
rmation; (8) accounting for the costs associated with
s order, which shall be reported to the Director of the

Information Security Oversight Office for publication; and(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Sec. 5.7. *Sanctions.* (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

PART 6 GENERAL—PROVISIONS

Sec. 6.1. *General Provisions.* (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended."Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, its officers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b) and 5.4(e) of this order.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

Sec. 6.2. *Effective Date.* This order shall become effective 180 days from the date of this order.

WILLIAM J. CLINTON

46-248 98 - 26

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Michael A. PULLARA, Plaintiff, v. CENTRAL INTELLIGENCE AGENCY Defendant.	)	Civ. Act. No. H 99 0587 [Proposed]

ORDER GRANTING SUMMARY JUDGMENT

This is an action under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (1994 & Supp. II 1996). Plaintiff submitted a FOIA request by letter dated November 4, 1997 seeking "information regarding the death of CIA Officer Fred Woodruff," an American citizen killed in Tbilisi, Georgia in 1993. By letter dated November 14, 1997, the Central Intelligence Agency ("CIA" or "Agency") acknowledged receipt of Plaintiff's FOIA request and assigned it a reference number. By letter dated July 31, 1998, CIA denied Plaintiff's FOIA request in full, pursuant to exemptions (b)(1) and (b)(3) of the FOIA.

CIA's July 31, 1998 letter neither confirmed nor denied the existence of records responsive to Plaintiff's FOIA request. In fact, CIA advised the Plaintiff that the fact of the existence or nonexistence of records responsive to Plaintiff's request was itself classified pursuant to the provisions of Executive Order 12958.

Plaintiff appealed CIA's denial of his FOIA request by letter dated August 11, 1998. CIA denied Plaintiff's appeal by letter dated December 22, 1998. Plaintiff's lawsuit followed. The administrative treatment of Plaintiff's FOIA request is more fully described in the Declaration of William H. McNair ("McNair Decl.") in support of Defendant's dispositive motion.

Executive Order 12958 (the "Order") governs proper classification of information and the treatment of properly classified information. Section 3.7(a) of the Order provides that any agency may refuse to confirm or deny the existence of records when that fact is, itself, classified. Information which is properly classified—such as the fact of the existence or non-existence of certain records under section 3.7(a) of the Order—is exempt from disclosure under FOIA exemption (b)(1). Accordingly, CIA properly denied Plaintiff's FOIA request pursuant to exemption (b)(1).

Furthermore, Plaintiff's FOIA request seeks information on intelligence sources and methods. Under the terms of the National Security Act, 50 U.S.C. § 403-3(c)(6), the Director of Central Intelligence ("DCI") is obligated to protect intelligence sources and methods from unauthorized disclosure. Section 403g of the Central Intelligence Agency Act protects from unauthorized disclosure the identities of CIA employees. These two Acts are "withholding statutes" for purposes of FOIA

exemption (b)(3), which exempts from disclosure under FOIA information "specifically exempted from disclosure by statute." Accordingly, CIA properly denied Plaintiff's FOIA request pursuant to FOIA exemption (b)(3).

The Court of Appeals for the Fifth Circuit has held that a District Court should be unwilling to "second guess" the determinations by the DCI in this area, absent a showing of bad faith. Knight v. CIA, 872 F.2d 660, 664 (5th Cir. 1989), cert. denied, 494 U.S. 1004 (1990), citing CIA v. Sims, 471 U.S. 159, 179 (1985)("The decisions of the DCI, who must, of course, be familiar with the whole picture, as judges are not, are worthy of great deference given the magnitude of the national security interests and the potential risks at stake."). This Court agrees and is unwilling to second guess the CIA's decision that it can neither admit nor deny the existence of the requested information.

Courts have upheld CIA's position in similar circumstances as are before the Court in this case. In Miller v. Casey, 730 F.2d 773 (D.C. Cir. 1984), the United States Court of Appeals for the District of Columbia Circuit upheld CIA's refusal, in response to a FOIA request, to confirm or deny the existence of records regarding alleged covert operations in Albania following World War II. The court held that "CIA's central premise—that an answer to whether the files existed would be tantamount to declaring whether the

mission occurred—is . . . sound." 730 F.2d at 776. Although the events in Albania were alleged to have occurred decades prior to the FOIA request—in contrast to the present case—the court found that "CIA's claim of foreseeable harm to the national security is all but indisputable." Id. at 777. These same considerations are at play in the current litigation and support summary judgment for the Agency.

The Supreme Court has held that both of these are "withholding statutes" for purposes of FOIA exemption (b)(3). CIA v. Sims, supra. The Supreme Court in Sims, noting the "wide-ranging authority" given to the DCI to protect intelligence sources and methods, held that it was "the responsibility of the DCI, not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk. . . ." Id. at 180. The United States Court of Appeals for the Fifth Circuit has stated unequivocally that "the FOIA simply does not apply to material the DCI specifically has exempted on the ground that it pertains to or could give rise to inferences about intelligence sources and methods." Knight, 872 F.2d at 664.

In this case, the CIA has determined that confirming or denying the existence of responsive records would divulge intelligence targeting, priorities and capabilities in a specific region of the world, as well as, depending on whether

CIA confirmed or denied the existence of records, intelligence sources and methods. McNair Decl. at ¶¶ 29-33. The Court will not second-guess this decision by the agency.

It is, therefore,

ORDERED that the defendant, the CIA, is entitled to summary judgment herein as a matter of law and this case is DISMISSED, with prejudice.

SIGNED this _____ day of _____, 1999, at Houston, Texas.

_____
UNITED STATES DISTRICT JUDGE